

REMARKS

Prior to this Reply, claims 42-82 were pending, of which claims 42, 69, and 77 are independent. In the Office Action, the Examiner rejected claims 42-82 under 35 U.S.C. § 102(e), as being anticipated by unpatentable over U.S. Patent Publication No. 2002/0012430 (*Lim*). In this response, Applicant amends claims 42, 69, and 77. Support for these amendments can be found in the originally-filed specification at, for example, page 6, lines 29-34, page 8, lines 1-5, and Figs. 1, 5 and 6. No new matter has been added. Accordingly, claims 42-82 are currently pending, of which claims 42, 69, and 77 are independent. Applicant respectfully traverses all pending rejections for at least the following reasons.¹

Rejection Under 35 U.S.C. § 102(e)

Applicant respectfully traverses the rejection of claims 42-82 under 35 U.S.C. § 102(e) as being anticipated by *Lim*. To properly establish that *Lim* anticipates Applicant's claims under 35 U.S.C. § 102, every element of each of the claims in issue must be found, either expressly described or under principles of inherency, in *Lim*. Furthermore, “[t]he identical invention must be shown in as complete detail as is contained in the ... claim.” M.P.E.P. § 2131 (quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1126, 1236, 9 U.S.P.Q.2d 1913, 1920 (Fed. Cir. 1989)).

¹ The Office Action contains a number of statements characterizing the Applicant's disclosure, including the claims, and the related art. Regardless of whether any such statement is specifically addressed herein, Applicant declines to automatically subscribe to any statement or characterization in the Office Action.

Representative amended independent claim 69 recites a block for secret-key-controlled cryptographic functions, operating on an input block of bits for generating an output block of bits comprising:

a multiplexer circuit that receives a first portion of bits of said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein the selected second set of key bits are output by said multiplexer circuit, said first portion of bits are transferred intact without modification by an encryption operation to an output of said building block, and the number of bits in the second set of key bits is less than the number of bits in the first set of key bits

Applicant respectfully submits that *Lim* does not teach or suggest at least this element of Applicant's amended independent claim 69.

Lim generally discloses "a pipelined encryption apparatus using data encryption standard algorithm." *Lim* ¶ [0001]. To that end, *Lim* discloses a macro encryption pipeline including three steps:

In a first step, 64-bit input data block is divided into eight 8-bit blocks, every four 8-bit blocks are sequentially inputted, gathered and stored into a left input buffer register (IBR(L)) 610 and a right input buffer register (IBR(R)) 620. In a second step, each 32-bit data block from the left and the right input buffer registers is alternatively inputted to first and second cipher function units and encrypted for 8 rounds. In a third step, each 32-bit data block is divided into four 8-bit blocks and outputted by 8-bit block through a left output buffer register (OBR(L)) 640 and a right output buffer register OBR(R)) 650.

Id. ¶ [0058].

As shown above, instead of disclosing "a block for secret-key-controlled cryptographic functions, operating on an input block of bits for generating an output block of bits comprising . . . a multiplexer circuit that receives a first portion of bits of

said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein . . . said first portion of bits are transferred intact without modification by an encryption operation to an output of said building block," as recited by amended independent claim 69, *Lim* discloses an encryption unit that encrypts all input bits and outputs them. Indeed, *Lim* discloses that its encryption unit receives a "64-bit input data block [that] is divided [into two 32-bit data blocks]. . . and stored into a left input buffer register (IBR(L)) 610 and a right input buffer register (IBR(R)) 620" and that "**each 32-bit data block . . . is alternatively inputted to first and second cipher function units and encrypted** for 8 rounds." *Lim* ¶ [0058] (emphasis added). These encrypted data blocks are "outputted [to] . . . left output buffer register (OBR(L)) 640 and a right output buffer register OBR(R)) 650." *Id.*

Because *Lim* discloses encrypting all data that gets input into its encryption apparatus, it does not teach or suggest "a block for secret-key-controlled cryptographic functions, operating on an input block of bits for generating an output block of bits comprising . . . a multiplexer circuit that receives a first portion of bits of said input block of bits and a first set of key bits as inputs, the first portion of said input block of bits operable to select a second set of key bits out of the first set of key bits, wherein . . . said first portion of bits are transferred intact without modification by an encryption operation to an output of said building block," as recited by amended claim 69.

Lim therefore fails to teach every element recited by amended independent claim 69. Thus, *Lim* cannot anticipate claim 69. Independent claims 42 and 77, although of

different scope, contain similar recitations as claim 69, and are patentably distinguishable from *Lim* for at least the same reasons. Claims 43-68, 70-76, and 78-82 depend from one of independent claims 42, 69, and 77 and, therefore, include all of the elements recited therein. The dependent claims are patentably distinguishable from *Lim* for at least the same reasons as claims 42, 69, and 77, and also recite additional elements that are neither taught nor suggested by *Lim*. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claims 42-82 under 35 U.S.C. § 102(e).

Conclusion

In view of the foregoing amendments and remarks, Applicant respectfully requests reconsideration and reexamination of this application and the timely allowance of the pending claims.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

By:



R. Bruce Bower
Reg. No. 37,099

Dated: August 27, 2010